UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/661,049	09/14/2000	Terence R. Spies	MS1 503US	8207

22801 7590 04/14/2004

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 04/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/661,049	SPIES, TERENCE R.	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-82 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-82 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 2, 17, and 32 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 2, 17, and 32, there is insufficient antecedent basis for "data" in these claims. Appropriate correction is required.

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 8, 11, 23, 26, 38, 41, 50, 53, 64, 67, 78 and 81 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claims 8, 23, 38, 50, 64 and 78 include the "generating at least a portion of the encryption key", "hashing at least a portion of the digitally signed second data" and "at least a portion of the third data". These subject matters are not described in the specification.

Claims 11, 26, 41, 53, 67 and 81 include the "substantially randomly generated". This subject matter is not described in the specification.

Claim Rejections - 35 USC § 102

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. Claims 1-11, 13-26, 28-41 and 43 are rejected under 35 U.S.C. 102(b) as being anticipated by Hardy et al. (6,079,018; hereinafter Hardy).

2. Regarding claims 1, 16 and 31, Hardy discloses a method for digitally signing a document with a digital signature that is unique and comprising:
Selectively hashing a first data string (see, for example, col. 8, lines 10-22; col. 10, lines 34-35; col. 12, lines 40-49);
Digitally signing a second data string (see, for example, col. 9, lines 32-33); and
Generating an encryption key based on the digitally signed second data string and a third data string (see, for example, col. 7, lines 60-67; col. 10, lines 20-30).

3. Regarding claims 2, 17, and 32, Hardy discloses:

Selectively encrypting data using the encryption key (see, for example, col. 1, line 61-col. 2, line 25; col. 9, lines 47-49).

4. Regarding claims 3-7, 18-22, and 33-37, Hardy discloses a non-volatile memory in a computer system that stores durably data including private key, other secret information and a hash value of a document (i.e., a data string) (see, for example, col. 9, lines 6-20; col. 9, lines 60-65; col. 13, lines 41-45).

5. Regarding claims 8-10, 23-25, and 38-40, Hardy discloses that a pseudo-random key is generated by cryptographically hashing combination (i.e., concatenation) of a document digest (corresponding to the recited the digitally signed second data) with another value (corresponding to the recited the third data string) (see, for example, col. 8, lines 8-13).

6. Regarding claims 11, 26, and 41, Hardy discloses a mechanism for selecting randomly a seed value for the computation of encryption key (see, for example, col. 6, lines 6-13).

7. Regarding claims 13-15, 28-30, and 43, Hardy discloses that a smart card as a portable device is suitable to be used for digitally signing a value in order to generate a signature (col. 7, lines 27-47).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 12-15, 27-29, and 42-82 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hardy et al. (6,079,018; hereinafter Hardy) in view of Epstein (6,453,416 B1).

9. Regarding claims 12, 27, 42, 44, 54, 58, 68, and 72, Hardy discloses a computer system (corresponding to the recited a first device) having modules that are configured to compute the hash value of a data string and generating an encryption key by combining a document digest (corresponding to the recited the digitally signed second data) with another value (corresponding to the recited the third data string) (see, for example, col. 8, lines 8-13; Fig. 2 blocks 142 and 146). But Hardy does not disclose the generation of data strings to be provided for computing the hash value and the encryption key. Epstein, however, teaches a secure signing device (for example, a smart card) and a method for using such a device to create a digital signature (col. 2, lines 29-39). In the Epstein method a number of data strings are provided by a computer system (corresponding to the recited generated or accessed by a first device) (abstract and col. 2, lines 66-67)

and hash of one of the data is computed (col. 2, lines 40-53). It would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the generation of a number of data items as taught in Epstein in the system of Hardy to be used in calculation of a hash value and generation of an encryption key, because it would provide for preventing the possibility that an imposter utilizes the signing device (i.e., smart card) (col. 2, lines 30-39).

10. Regarding claims 13-15, 28-29, 43, 55-57, 69-71 and 82, Epstein discloses a signing device such as a smart card that digitally signs a value and generate a signature, for example, of a document to be authenticated (col. 2, lines 30-54).

11. Regarding claims 45-47, 59-61 and 73-75, Epstein discloses that after receiving (corresponding to the recited accessing) data, the data is decrypted using an encryption key (see, for example, col. 6, lines 12-20) and the result of the decryption is a hash value.

12. Regarding claims 48, 49, 62, 63, 76 and 77, Epstein discloses a memory system that the provided data strings are read from (see, for example Fig. 1, block 146).

13. Regarding claims 50-52, 64-66 and 78-80, Hardy discloses that a pseudo-random key is generated by cryptographically hashing combination (i.e., concatenation) of a document digest (corresponding to the recited the digitally

signed second data) with another value (corresponding to the recited the third data string) (see, for example, col. 8, lines 8-13).

14. Regarding claims 53, 67 and 81, Hardy discloses a mechanism for selecting randomly a seed value for the computation of encryption key (see, for example, col. 6, lines 6-13).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patent No. 6,357,004 B1 to Davis

US Patent No. 6,484,259 B1 to Barlow

US Patent No. 5,689,565 to Spies et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 703-305-8074. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

A.M.

Abdulhakim Nobahar
Examiner
Art Unit 2132

AN
April 8, 2004

Gilberto Barron

GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100